FIG.1

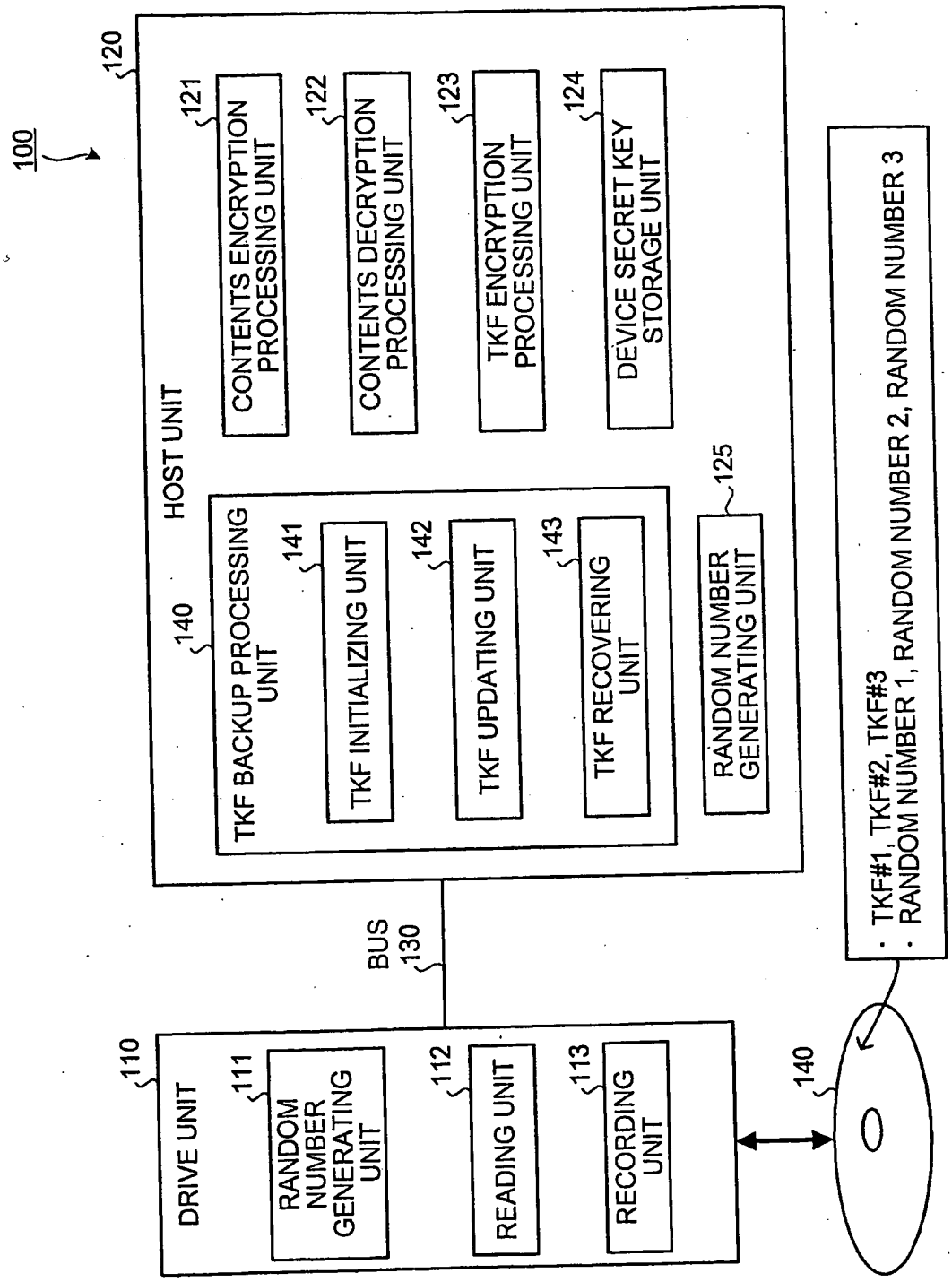

100
120
HOST UNIT
121
CONTENTS ENCRYPTION PROCESSING UNIT
122
CONTENTS DECRYPTION PROCESSING UNIT
123
TKF ENCRYPTION PROCESSING UNIT
124
DEVICE SECRET KEY STORAGE UNIT
140
TKF BACKUP PROCESSING UNIT
141
TKF INITIALIZING UNIT
142
TKF UPDATING UNIT
143
TKF RECOVERING UNIT
125
RANDOM NUMBER GENERATING UNIT
BUS
130
110
DRIVE UNIT
111
RANDOM NUMBER GENERATING UNIT
112
READING UNIT
113
RECORDING UNIT
140
· TKF#1, TKF#2, TKF#3
· RANDOM NUMBER 1, RANDOM NUMBER 2, RANDOM NUMBER 3

FIG.2

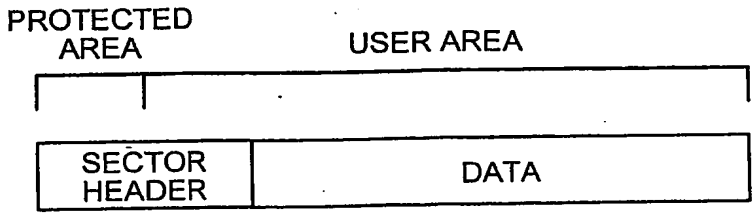

PROTECTED AREA
USER AREA
SECTOR HEADER
DATA

FIG.3

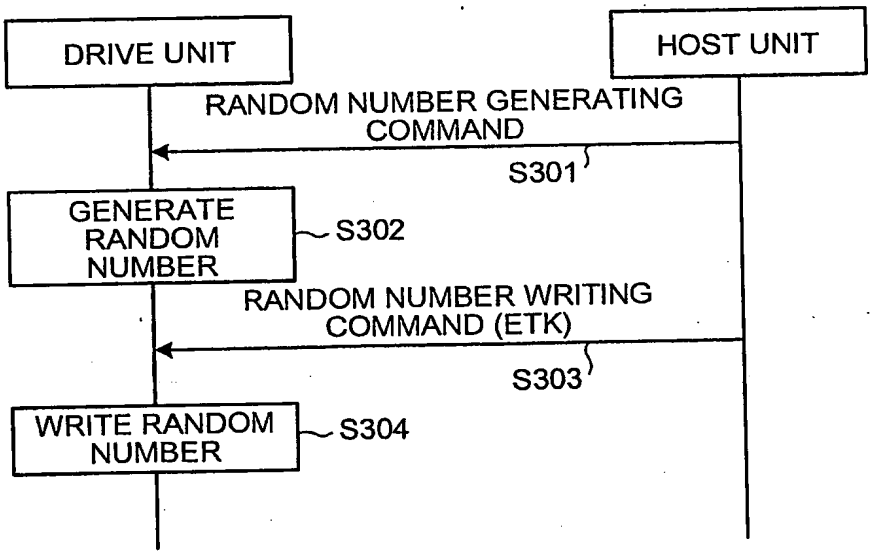
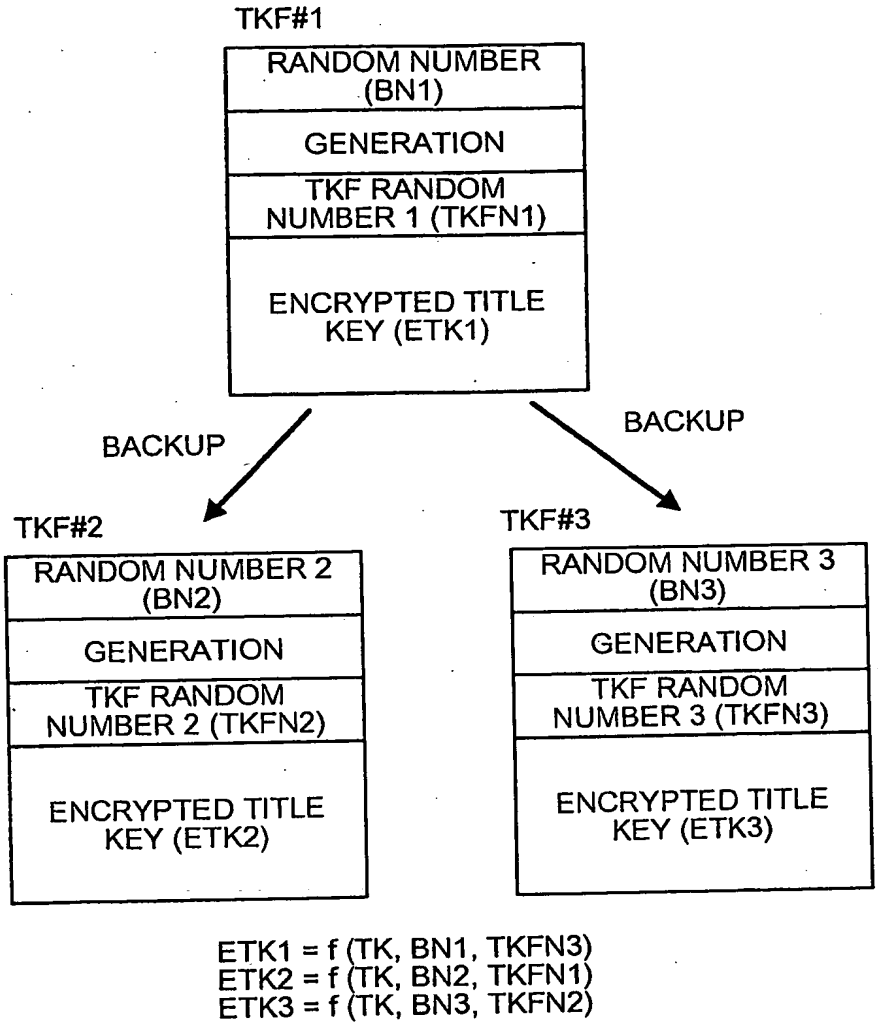

DRIVE UNIT
HOST UNIT
RANDOM NUMBER GENERATING COMMAND
S301
GENERATE RANDOM NUMBER
S302
RANDOM NUMBER WRITING COMMAND (ETK)
S303
WRITE RANDOM NUMBER
S304

FIG.4A



ETK1 = f (TK, BN1, TKFN3)
ETK2 = f (TK, BN2, TKFN1)
ETK3 = f (TK, BN3, TKFN2)

FIG.4B

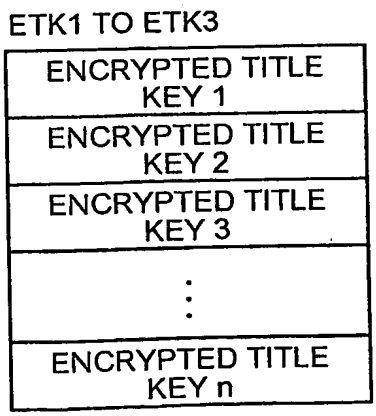


FIG.5

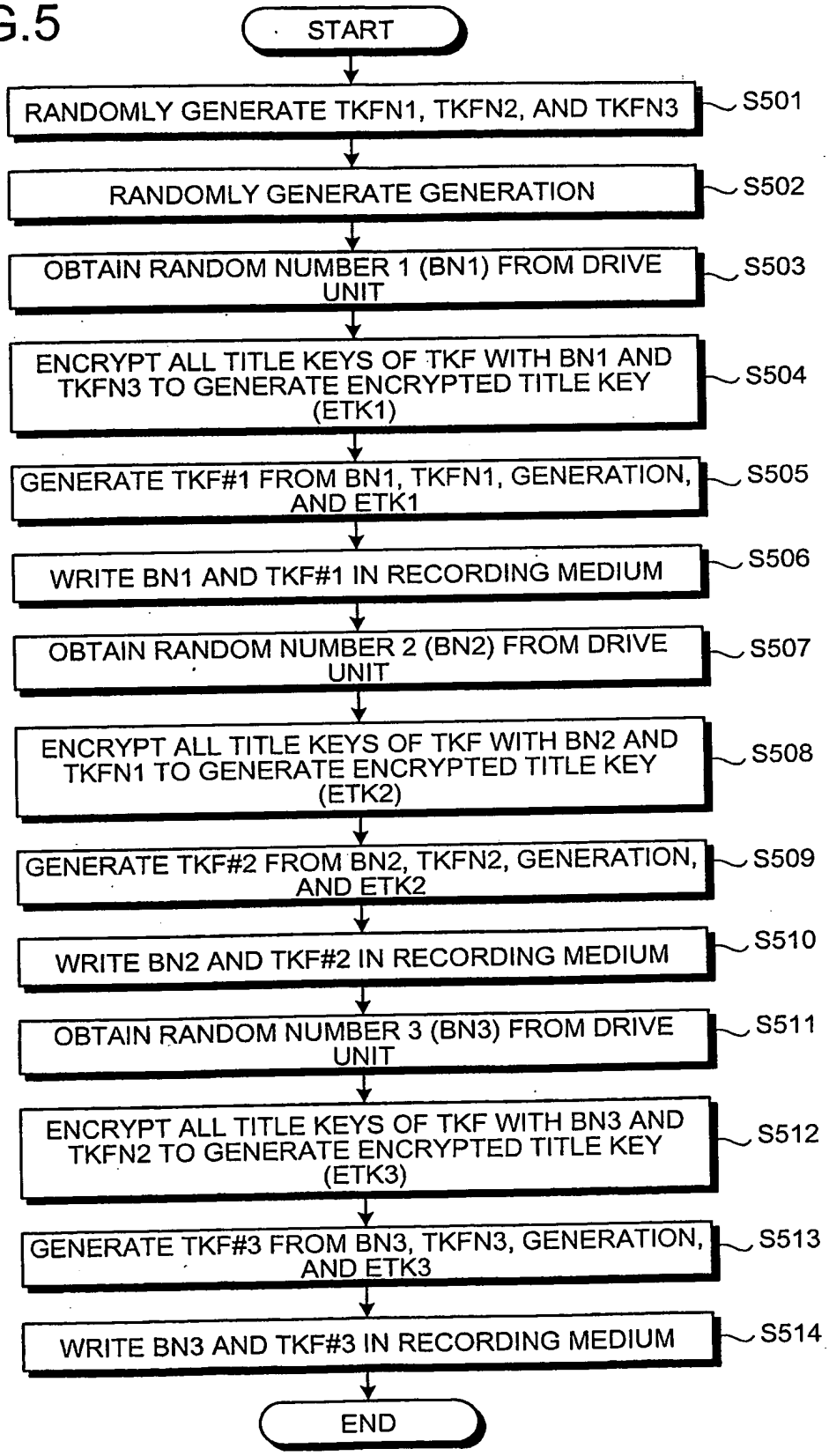

START
RANDOMLY GENERATE TKFN1, TKFN2, AND TKFN3
S501
RANDOMLY GENERATE GENERATION
S502
OBTAIN RANDOM NUMBER 1 (BN1) FROM DRIVE UNIT
S503
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN3 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S504
GENERATE TKF#1 FROM BN1, TKFN1, GENERATION, AND ETK1
S505
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S506
OBTAIN RANDOM NUMBER 2 (BN2) FROM DRIVE UNIT
S507
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S508
GENERATE TKF#2 FROM BN2, TKFN2, GENERATION, AND ETK2
S509
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S510
OBTAIN RANDOM NUMBER 3 (BN3) FROM DRIVE UNIT
S511
ENCRYPT ALL TITLE KEYS OF TKF WITH BN3 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK3)
S512
GENERATE TKF#3 FROM BN3, TKFN3, GENERATION, AND ETK3
S513
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S514
END

FIG.6A

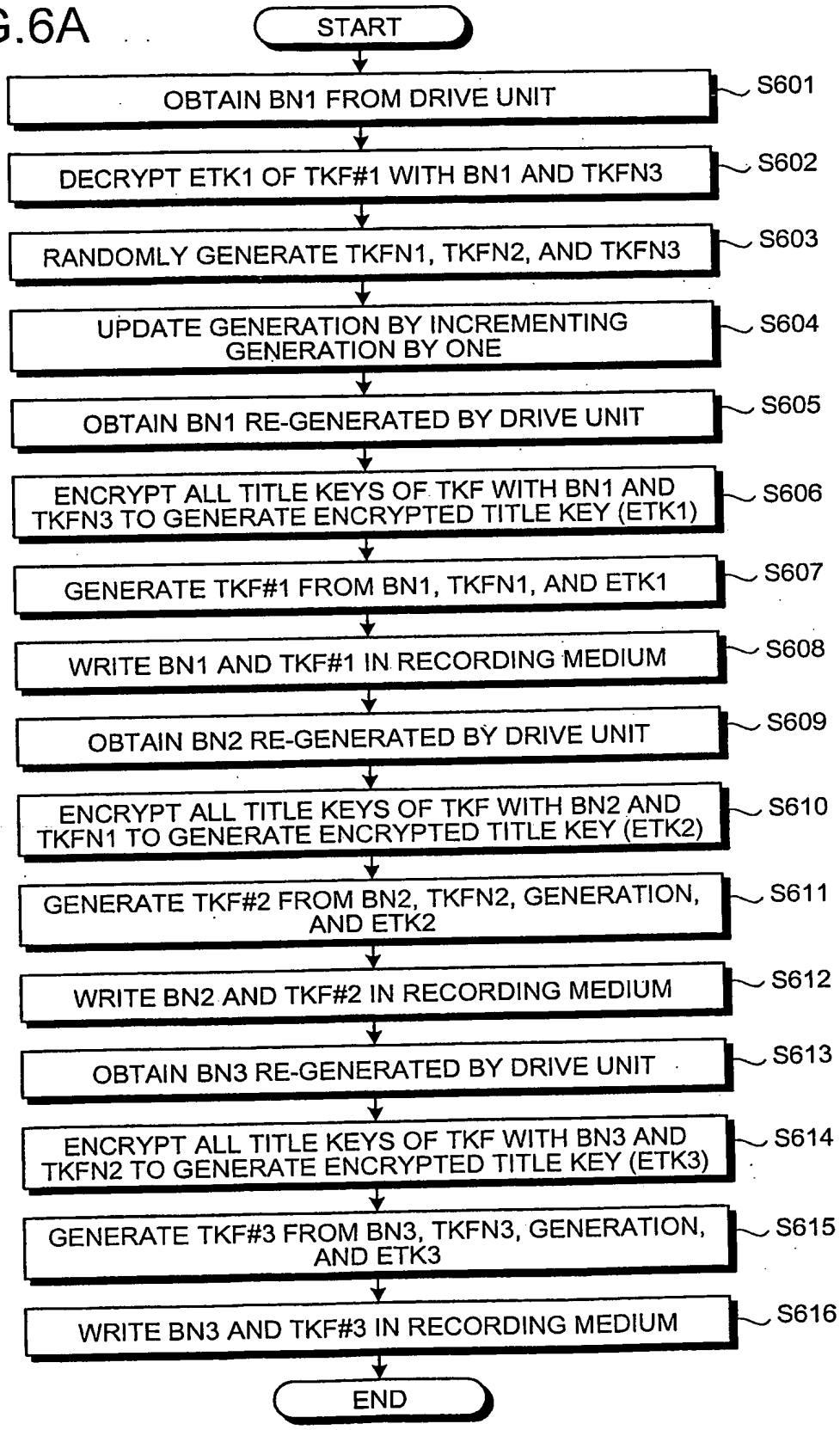

START
OBTAIN BN1 FROM DRIVE UNIT
S601
DECRYPT ETK1 OF TKF#1 WITH BN1 AND TKFN3
S602
RANDOMLY GENERATE TKFN1, TKFN2, AND TKFN3
S603
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S604
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S605
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN3 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S606
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S607
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S608
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S609
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S610
GENERATE TKF#2 FROM BN2, TKFN2, GENERATION, AND ETK2
S611
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S612
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S613
ENCRYPT ALL TITLE KEYS OF TKF WITH BN3 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK3)
S614
GENERATE TKF#3 FROM BN3, TKFN3, GENERATION, AND ETK3
S615
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S616
END

FIG.6B

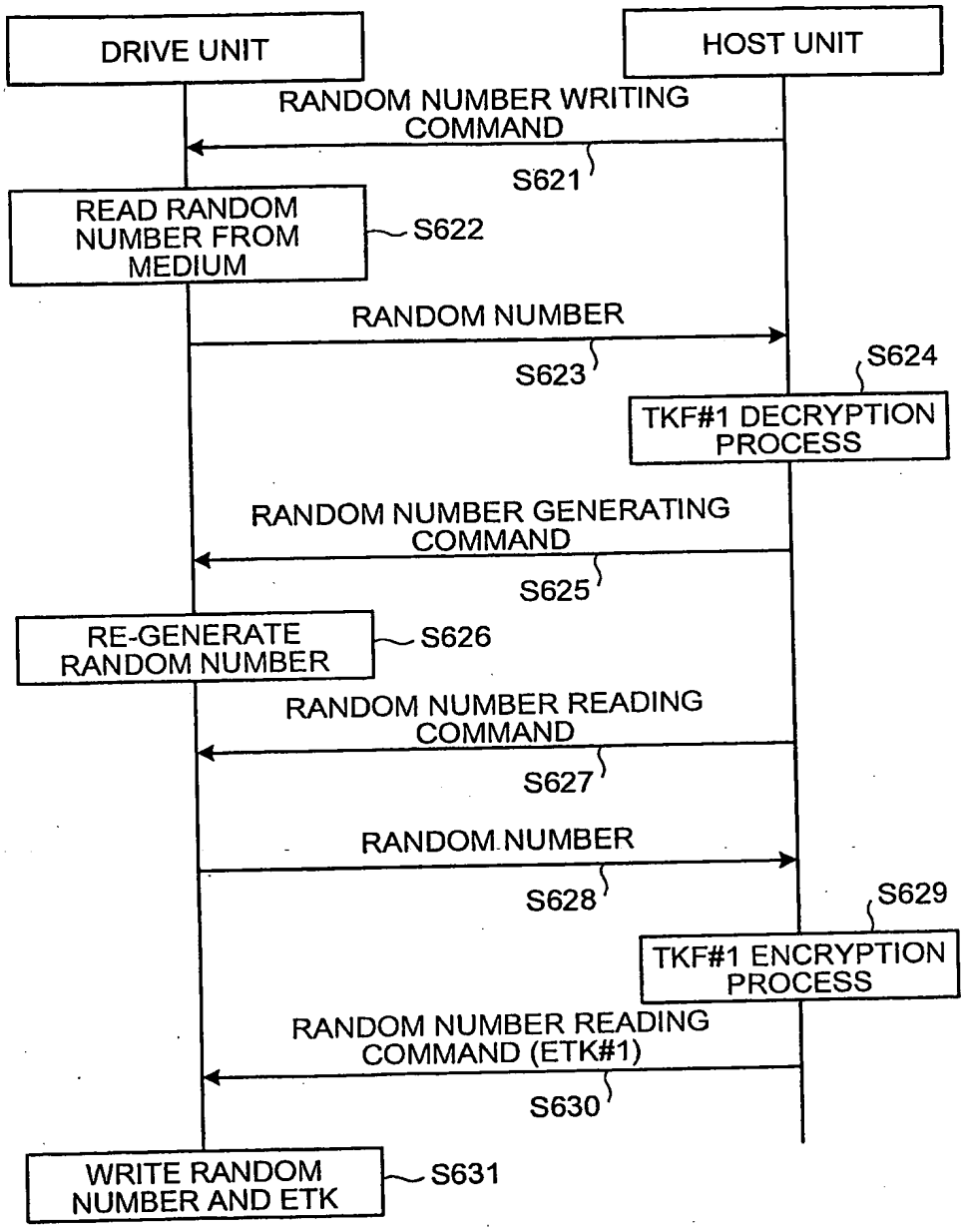

DRIVE UNIT
HOST UNIT
RANDOM NUMBER WRITING COMMAND
S621
READ RANDOM NUMBER FROM MEDIUM
S622
RANDOM NUMBER
S623
S624
TKF#1 DECRYPTION PROCESS
RANDOM NUMBER GENERATING COMMAND
S625
RE-GENERATE RANDOM NUMBER
S626
RANDOM NUMBER READING COMMAND
S627
RANDOM NUMBER
S628
S629
TKF#1 ENCRYPTION PROCESS
RANDOM NUMBER READING COMMAND (ETK#1)
S630
WRITE RANDOM NUMBER AND ETK
S631

FIG.7

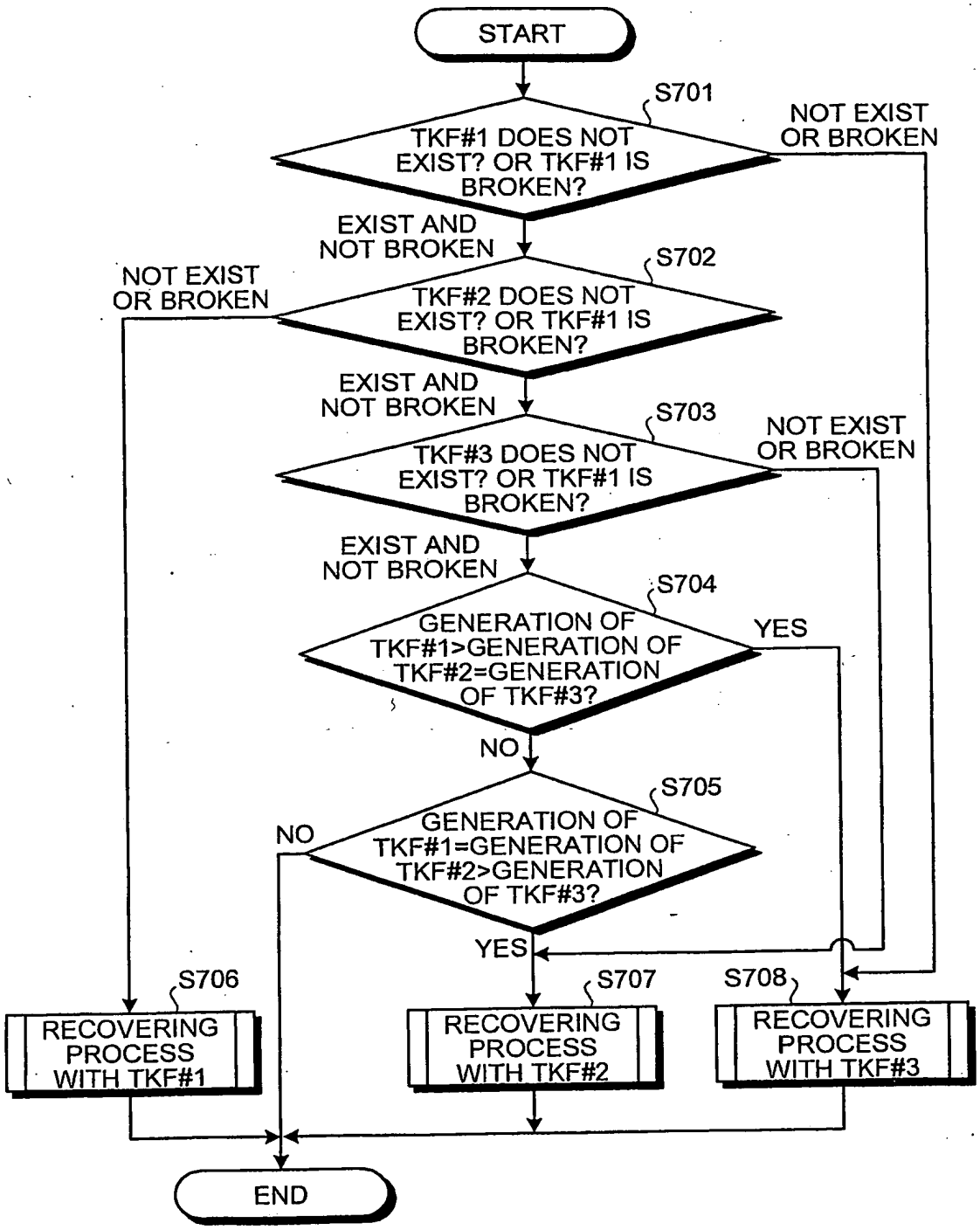

START
S701
TKF#1 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S702
TKF#2 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S703
TKF#3 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S704
GENERATION OF TKF#1>GENERATION OF TKF#2=GENERATION OF TKF#3?
YES
NO
S705
GENERATION OF TKF#1=GENERATION OF TKF#2>GENERATION OF TKF#3?
NO
YES
S706
RECOVERING PROCESS WITH TKF#1
S707
RECOVERING PROCESS WITH TKF#2
S708
RECOVERING PROCESS WITH TKF#3
END

FIG.8

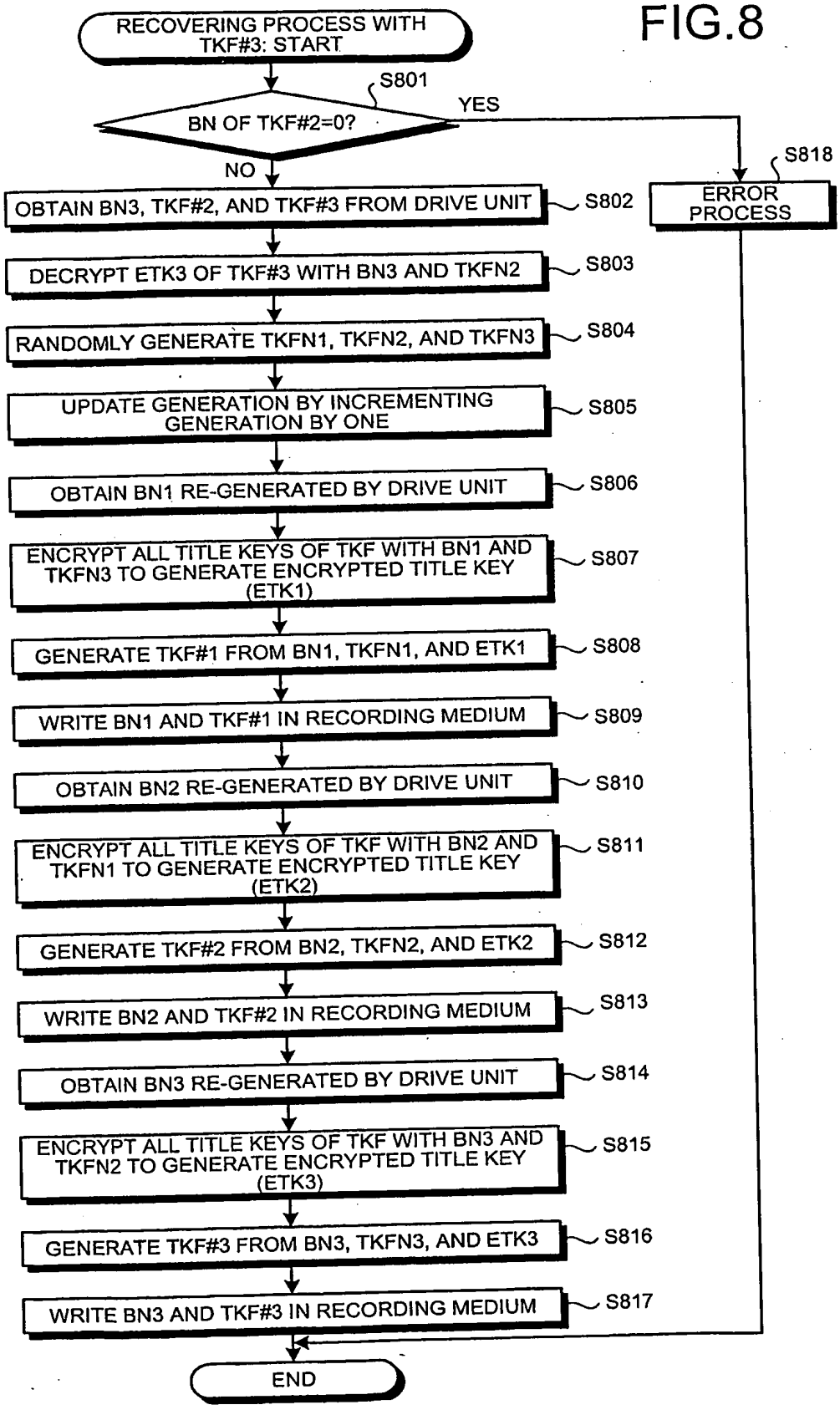

RECOVERING PROCESS WITH TKF#3: START
S801
BN OF TKF#2=0?
YES
NO
S818
ERROR PROCESS
OBTAIN BN3, TKF#2, AND TKF#3 FROM DRIVE UNIT
S802
DECRYPT ETK3 OF TKF#3 WITH BN3 AND TKFN2
S803
RANDOMLY GENERATE TKFN1, TKFN2, AND TKFN3
S804
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S805
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S806
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN3 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S807
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S808
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S809
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S810
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S811
GENERATE TKF#2 FROM BN2, TKFN2, AND ETK2
S812
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S813
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S814
ENCRYPT ALL TITLE KEYS OF TKF WITH BN3 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK3)
S815
GENERATE TKF#3 FROM BN3, TKFN3, AND ETK3
S816
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S817
END

FIG.9

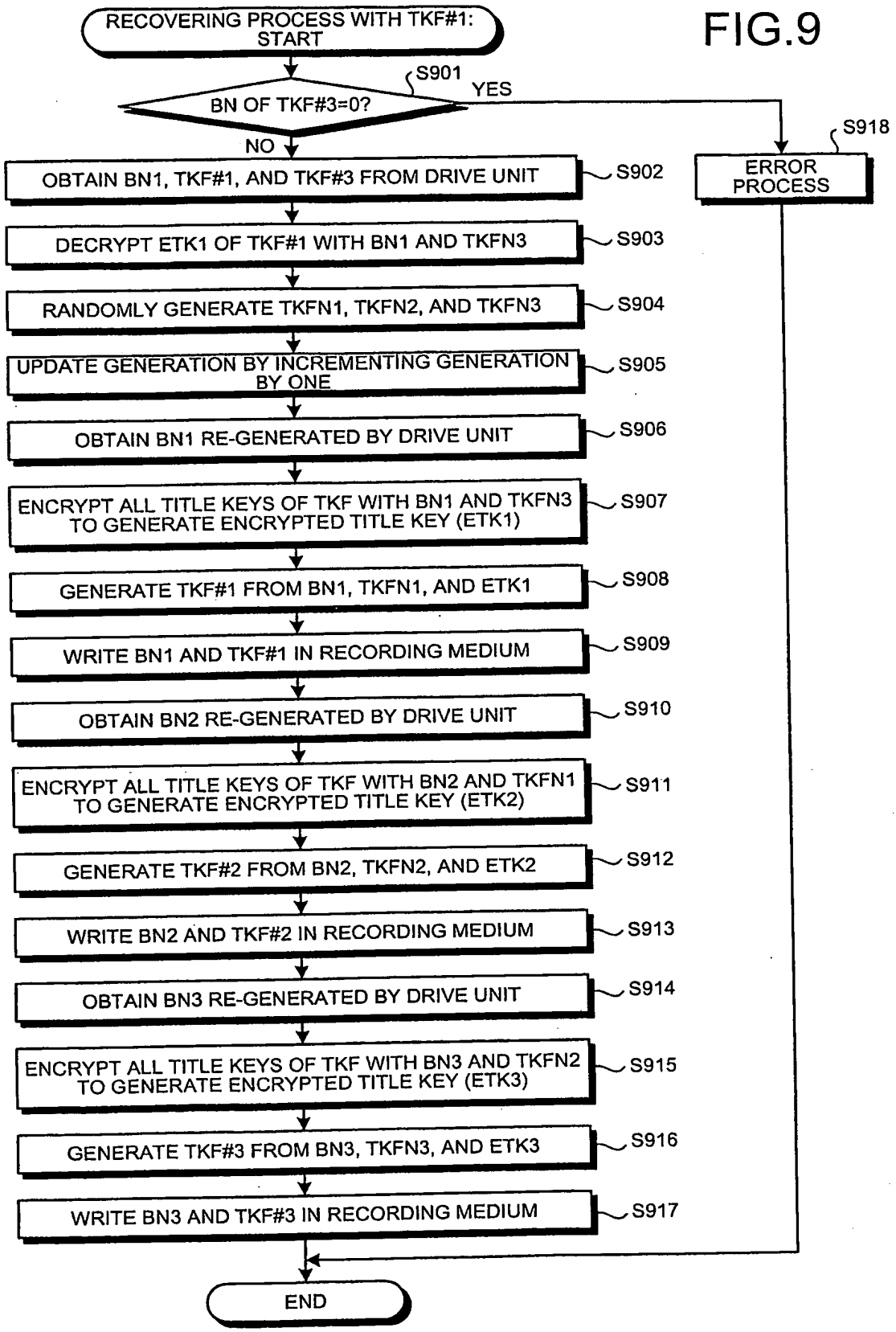

RECOVERING PROCESS WITH TKF#1: START
S901
BN OF TKF#3=0?
YES
NO
S918
ERROR PROCESS
OBTAIN BN1, TKF#1, AND TKF#3 FROM DRIVE UNIT
S902
DECRYPT ETK1 OF TKF#1 WITH BN1 AND TKFN3
S903
RANDOMLY GENERATE TKFN1, TKFN2, AND TKFN3
S904
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S905
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S906
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN3 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S907
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S908
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S909
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S910
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S911
GENERATE TKF#2 FROM BN2, TKFN2, AND ETK2
S912
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S913
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S914
ENCRYPT ALL TITLE KEYS OF TKF WITH BN3 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK3)
S915
GENERATE TKF#3 FROM BN3, TKFN3, AND ETK3
S916
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S917
END

FIG.10

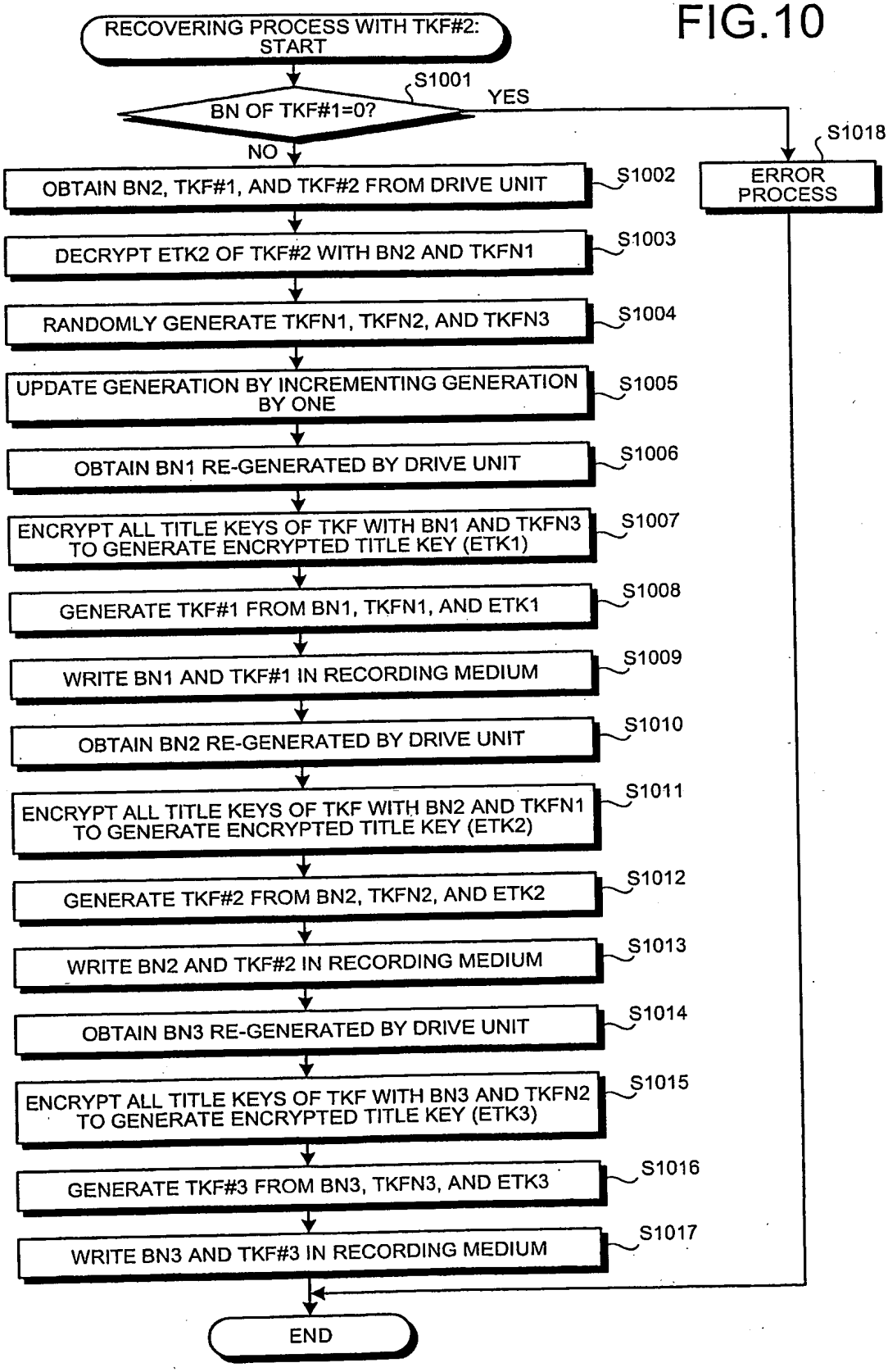

RECOVERING PROCESS WITH TKF#2: START
S1001
BN OF TKF#1=0?
YES
NO
S1018
ERROR PROCESS
OBTAIN BN2, TKF#1, AND TKF#2 FROM DRIVE UNIT
S1002
DECRYPT ETK2 OF TKF#2 WITH BN2 AND TKFN1
S1003
RANDOMLY GENERATE TKFN1, TKFN2, AND TKFN3
S1004
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S1005
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S1006
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN3 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S1007
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S1008
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S1009
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S1010
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S1011
GENERATE TKF#2 FROM BN2, TKFN2, AND ETK2
S1012
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S1013
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S1014
ENCRYPT ALL TITLE KEYS OF TKF WITH BN3 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK3)
S1015
GENERATE TKF#3 FROM BN3, TKFN3, AND ETK3
S1016
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1017
END

FIG.11

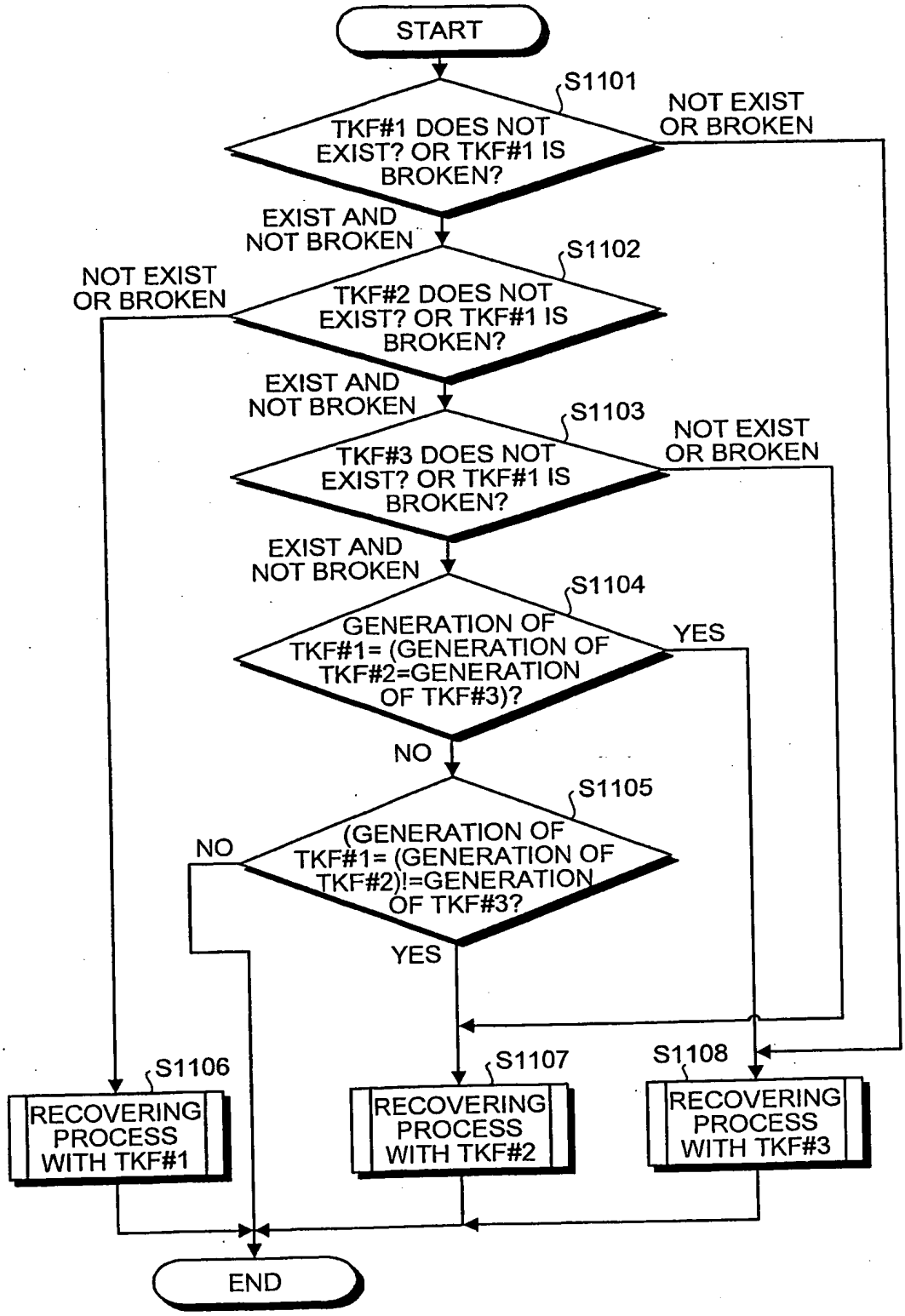

START
S1101
TKF#1 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1102
TKF#2 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1103
TKF#3 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1104
GENERATION OF TKF#1= (GENERATION OF TKF#2=GENERATION OF TKF#3)?
YES
NO
S1105
(GENERATION OF TKF#1= (GENERATION OF TKF#2)!=GENERATION OF TKF#3?
NO
YES
S1106
RECOVERING PROCESS WITH TKF#1
S1107
RECOVERING PROCESS WITH TKF#2
S1108
RECOVERING PROCESS WITH TKF#3
END

FIG.12

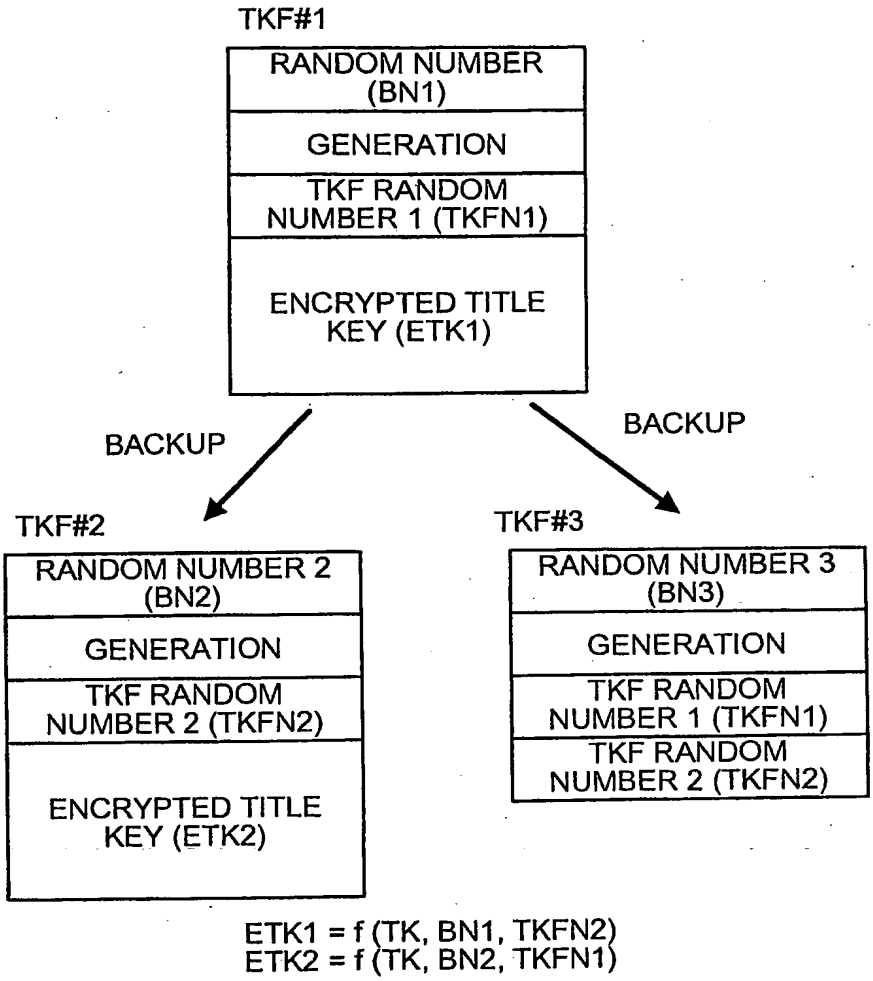

TKF#1
RANDOM NUMBER (BN1)
GENERATION
TKF RANDOM NUMBER 1 (TKFN1)
ENCRYPTED TITLE KEY (ETK1)
BACKUP
BACKUP
TKF#2
RANDOM NUMBER 2 (BN2)
GENERATION
TKF RANDOM NUMBER 2 (TKFN2)
ENCRYPTED TITLE KEY (ETK2)
TKF#3
RANDOM NUMBER 3 (BN3)
GENERATION
TKF RANDOM NUMBER 1 (TKFN1)
TKF RANDOM NUMBER 2 (TKFN2)
ETK1 = f (TK, BN1, TKFN2)
ETK2 = f (TK, BN2, TKFN1)

FIG.13

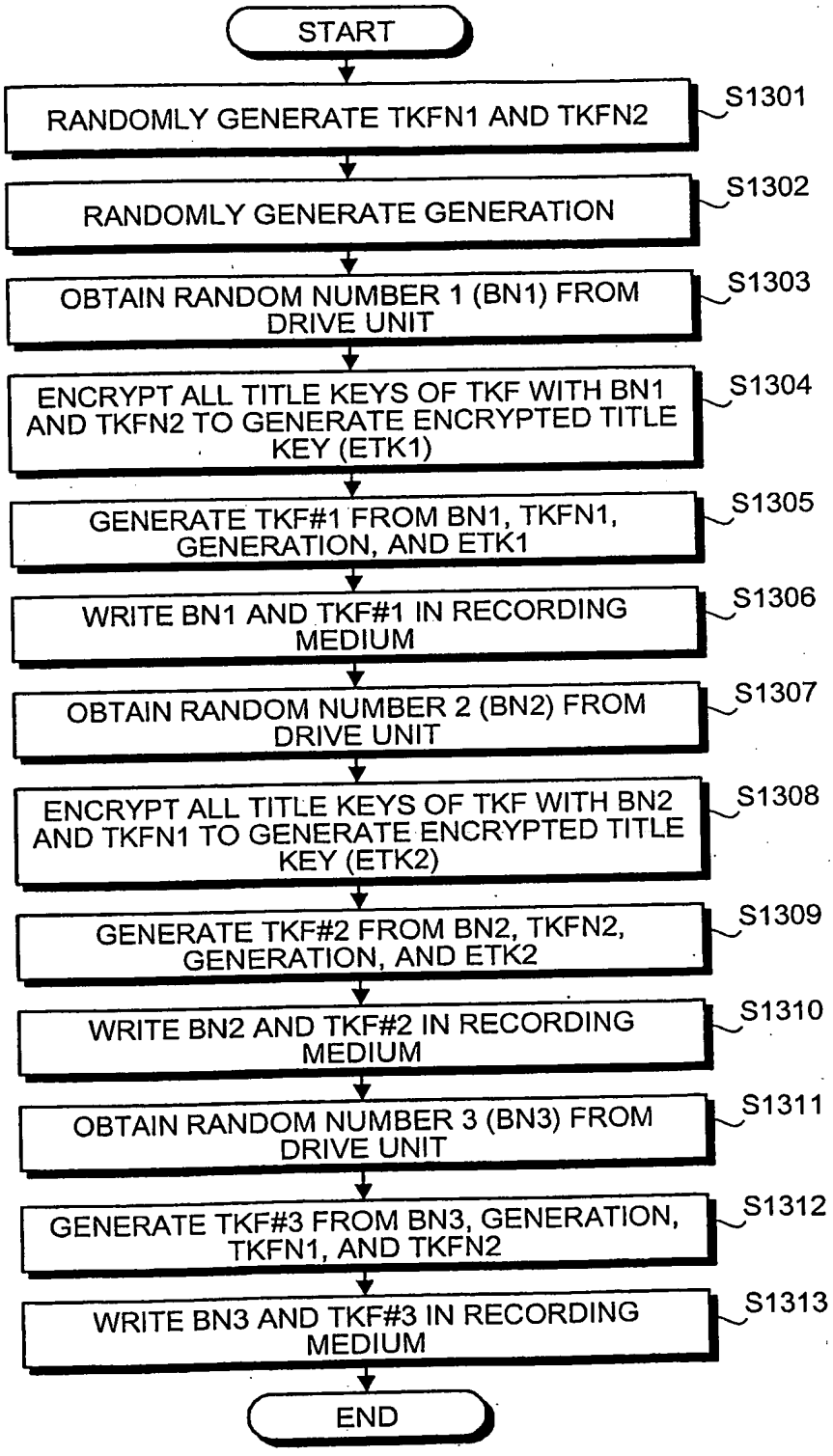

START
RANDOMLY GENERATE TKFN1 AND TKFN2
S1301
RANDOMLY GENERATE GENERATION
S1302
OBTAIN RANDOM NUMBER 1 (BN1) FROM DRIVE UNIT
S1303
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S1304
GENERATE TKF#1 FROM BN1, TKFN1, GENERATION, AND ETK1
S1305
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S1306
OBTAIN RANDOM NUMBER 2 (BN2) FROM DRIVE UNIT
S1307
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S1308
GENERATE TKF#2 FROM BN2, TKFN2, GENERATION, AND ETK2
S1309
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S1310
OBTAIN RANDOM NUMBER 3 (BN3) FROM DRIVE UNIT
S1311
GENERATE TKF#3 FROM BN3, GENERATION, TKFN1, AND TKFN2
S1312
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1313
END

FIG.14

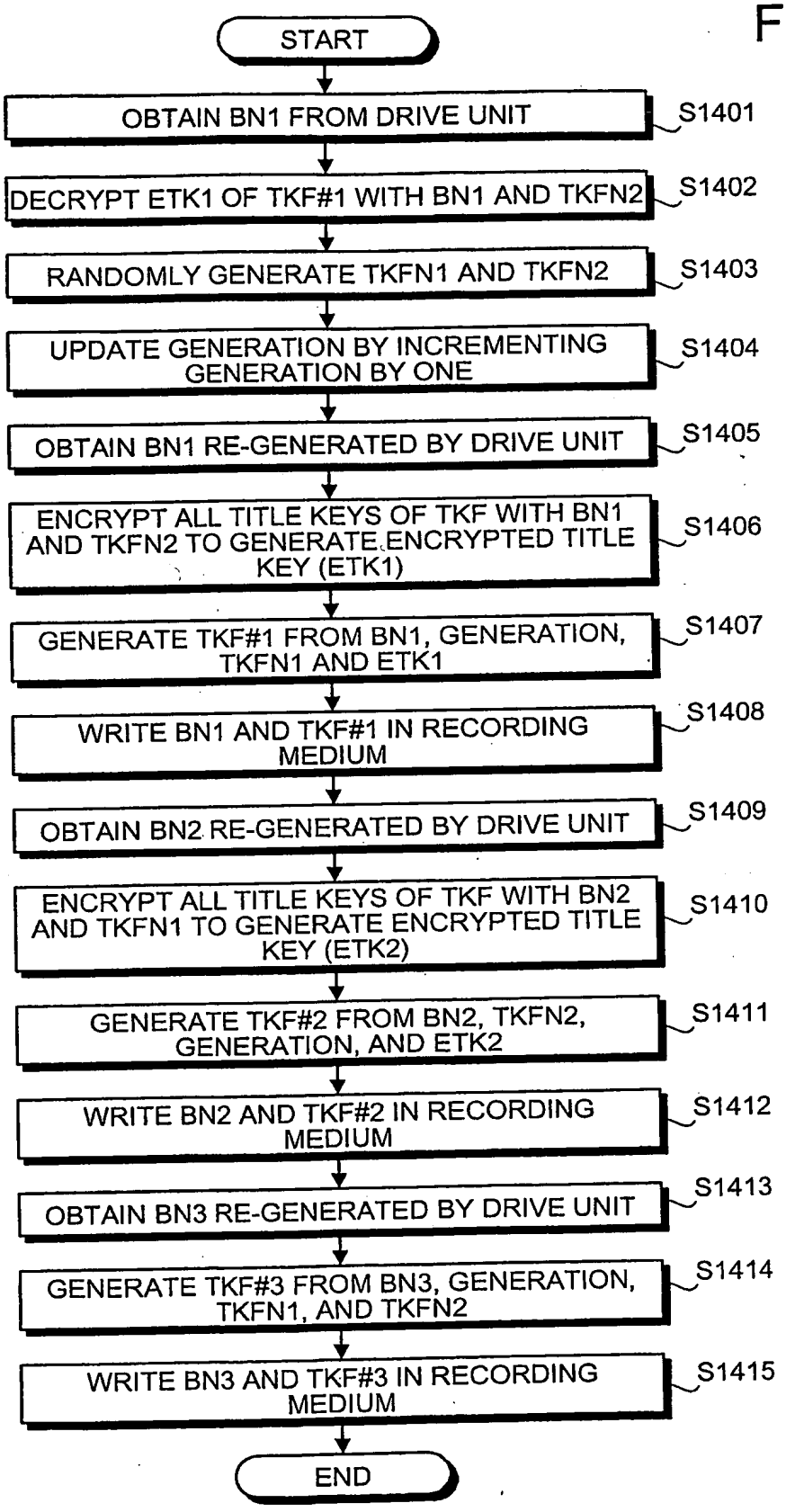

START
OBTAIN BN1 FROM DRIVE UNIT
S1401
DECRYPT ETK1 OF TKF#1 WITH BN1 AND TKFN2
S1402
RANDOMLY GENERATE TKFN1 AND TKFN2
S1403
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S1404
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S1405
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S1406
GENERATE TKF#1 FROM BN1, GENERATION, TKFN1 AND ETK1
S1407
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S1408
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S1409
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S1410
GENERATE TKF#2 FROM BN2, TKFN2, GENERATION, AND ETK2
S1411
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S1412
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S1413
GENERATE TKF#3 FROM BN3, GENERATION, TKFN1, AND TKFN2
S1414
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1415
END

FIG.15

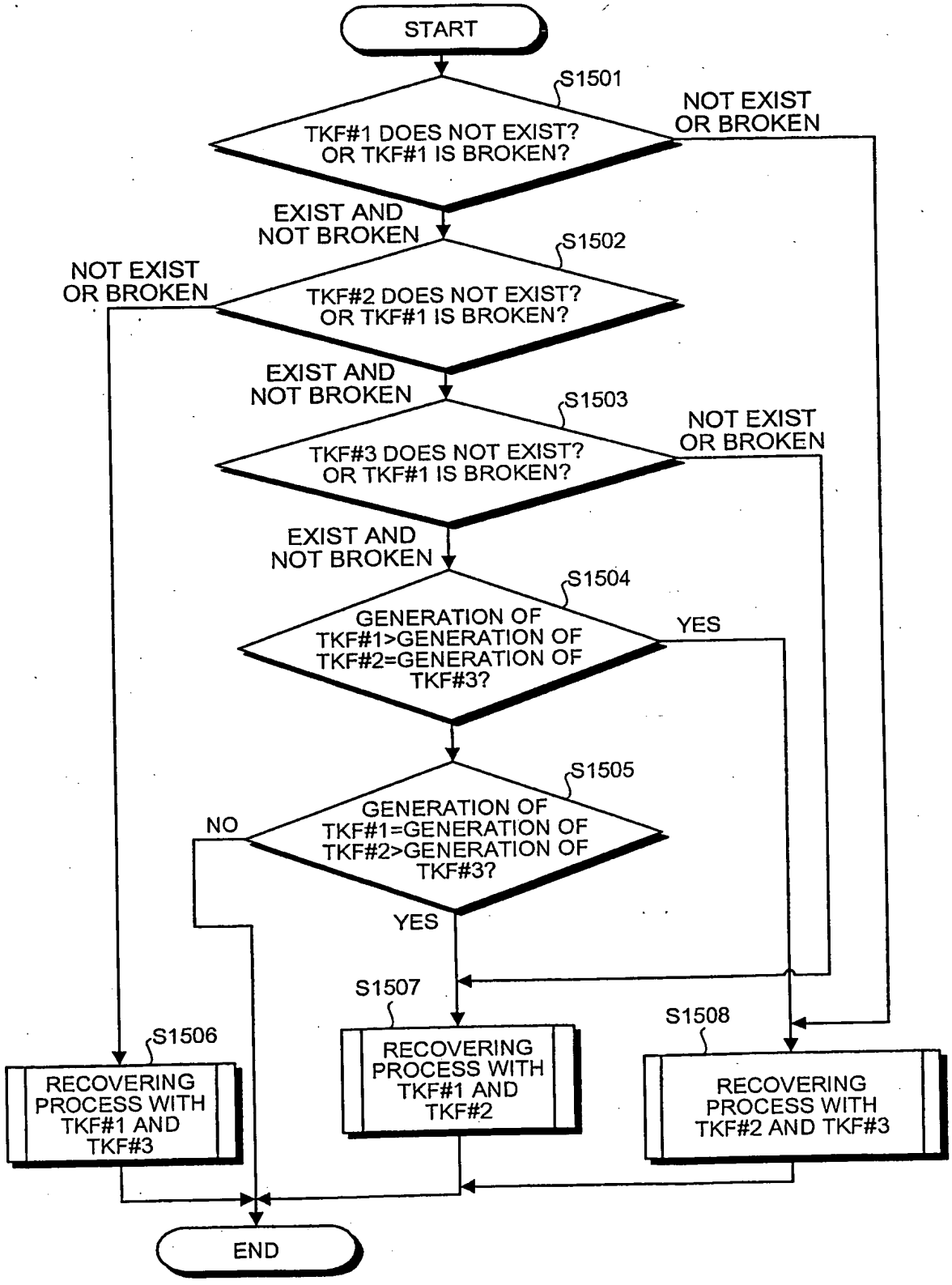

START
S1501
TKF#1 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1502
TKF#2 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1503
TKF#3 DOES NOT EXIST? OR TKF#1 IS BROKEN?
NOT EXIST OR BROKEN
EXIST AND NOT BROKEN
S1504
GENERATION OF TKF#1>GENERATION OF TKF#2=GENERATION OF TKF#3?
YES
S1505
GENERATION OF TKF#1=GENERATION OF TKF#2>GENERATION OF TKF#3?
NO
YES
S1506
RECOVERING PROCESS WITH TKF#1 AND TKF#3
S1507
RECOVERING PROCESS WITH TKF#1 AND TKF#2
S1508
RECOVERING PROCESS WITH TKF#2 AND TKF#3
END

FIG.16

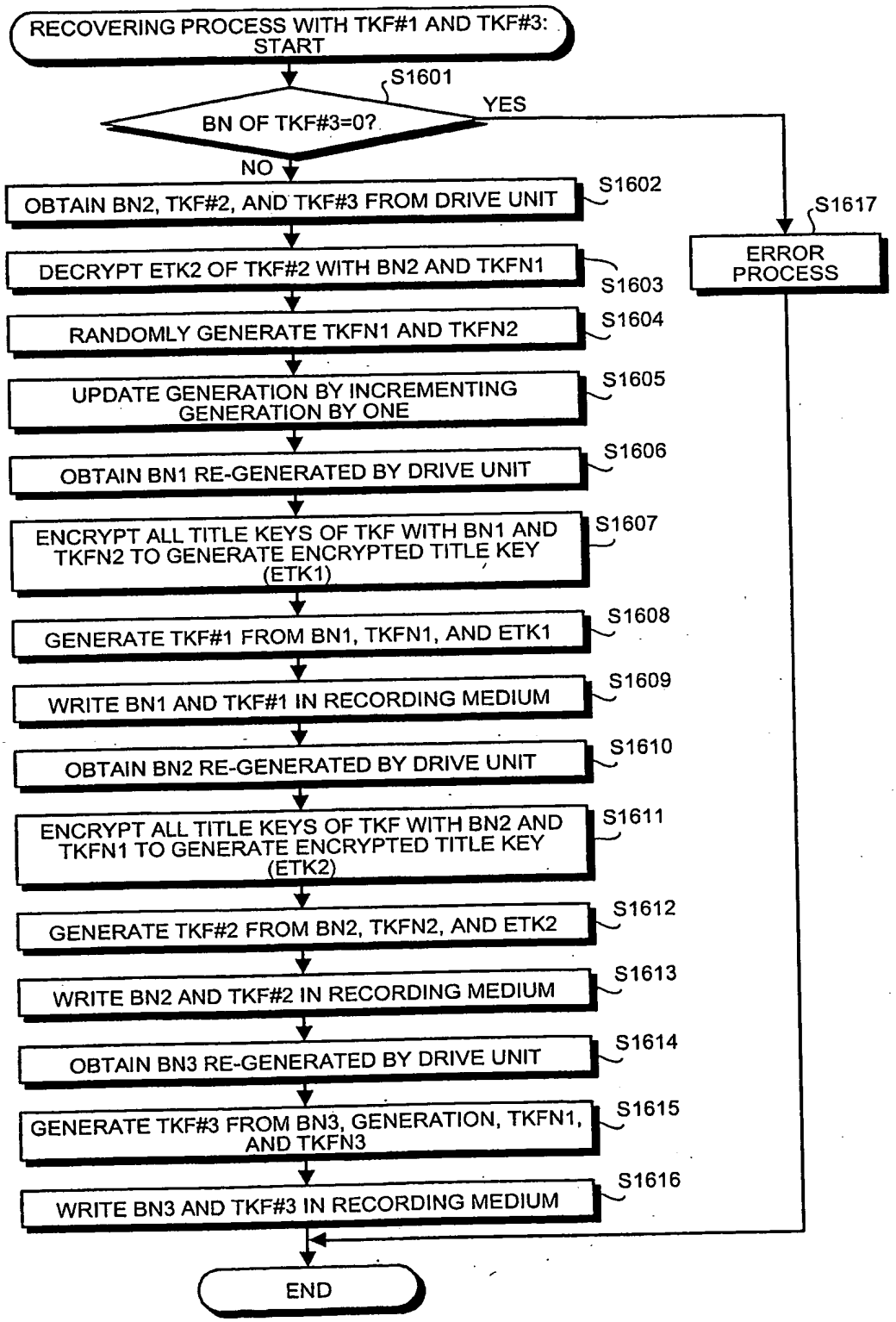

RECOVERING PROCESS WITH TKF#1 AND TKF#3: START
S1601
BN OF TKF#3=0?
YES
NO
S1602
OBTAIN BN2, TKF#2, AND TKF#3 FROM DRIVE UNIT
S1603
DECRYPT ETK2 OF TKF#2 WITH BN2 AND TKFN1
S1604
RANDOMLY GENERATE TKFN1 AND TKFN2
S1605
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S1606
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S1607
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S1608
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S1609
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S1610
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S1611
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S1612
GENERATE TKF#2 FROM BN2, TKFN2, AND ETK2
S1613
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S1614
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S1615
GENERATE TKF#3 FROM BN3, GENERATION, TKFN1, AND TKFN3
S1616
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1617
ERROR PROCESS
END

FIG.17

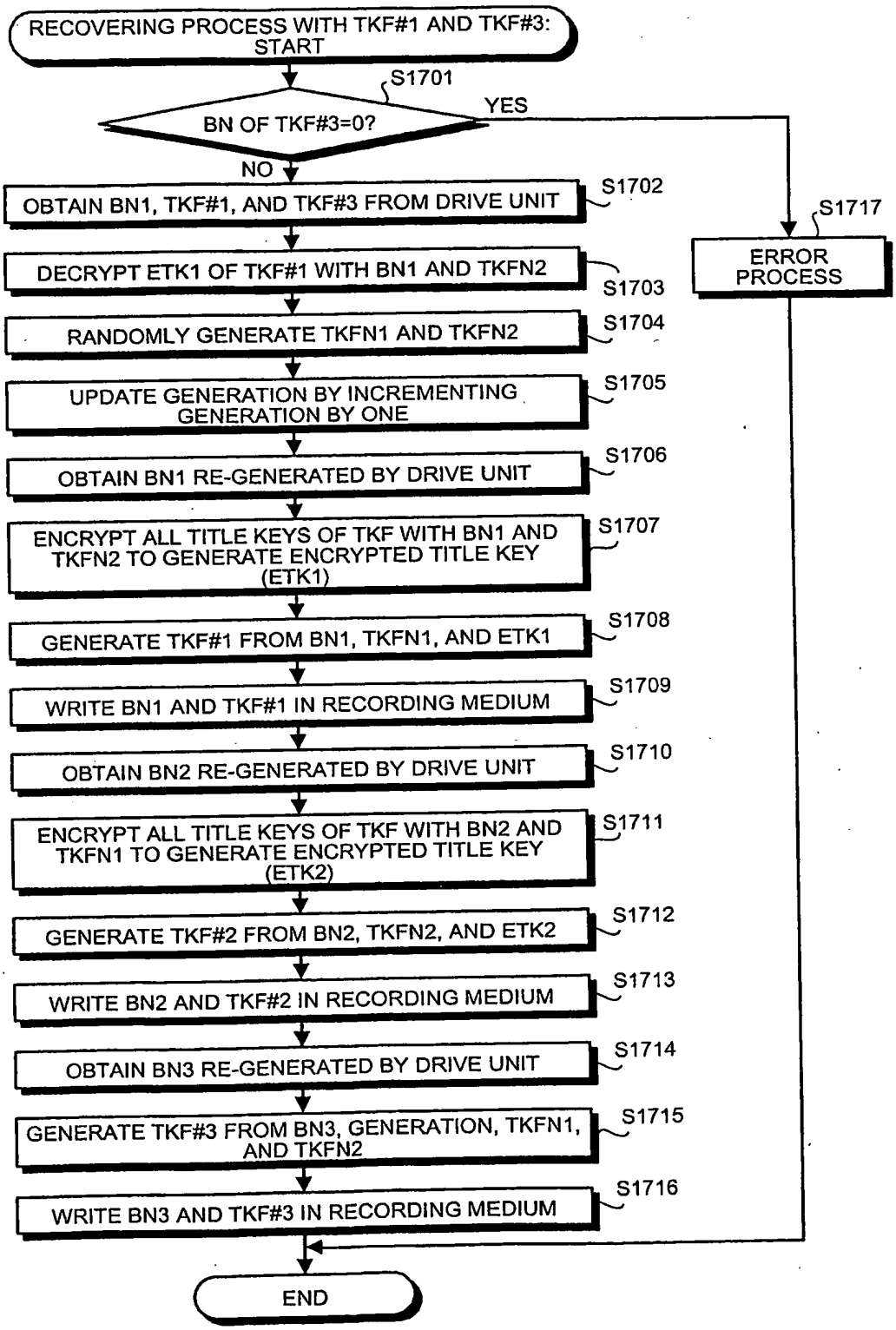

RECOVERING PROCESS WITH TKF#1 AND TKF#3: START
S1701
BN OF TKF#3=0?
YES
NO
S1717
ERROR PROCESS
OBTAIN BN1, TKF#1, AND TKF#3 FROM DRIVE UNIT
S1702
DECRYPT ETK1 OF TKF#1 WITH BN1 AND TKFN2
S1703
RANDOMLY GENERATE TKFN1 AND TKFN2
S1704
UPDATE GENERATION BY INCREMENTING GENERATION BY ONE
S1705
OBTAIN BN1 RE-GENERATED BY DRIVE UNIT
S1706
ENCRYPT ALL TITLE KEYS OF TKF WITH BN1 AND TKFN2 TO GENERATE ENCRYPTED TITLE KEY (ETK1)
S1707
GENERATE TKF#1 FROM BN1, TKFN1, AND ETK1
S1708
WRITE BN1 AND TKF#1 IN RECORDING MEDIUM
S1709
OBTAIN BN2 RE-GENERATED BY DRIVE UNIT
S1710
ENCRYPT ALL TITLE KEYS OF TKF WITH BN2 AND TKFN1 TO GENERATE ENCRYPTED TITLE KEY (ETK2)
S1711
GENERATE TKF#2 FROM BN2, TKFN2, AND ETK2
S1712
WRITE BN2 AND TKF#2 IN RECORDING MEDIUM
S1713
OBTAIN BN3 RE-GENERATED BY DRIVE UNIT
S1714
GENERATE TKF#3 FROM BN3, GENERATION, TKFN1, AND TKFN2
S1715
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1716
END

FIG.18

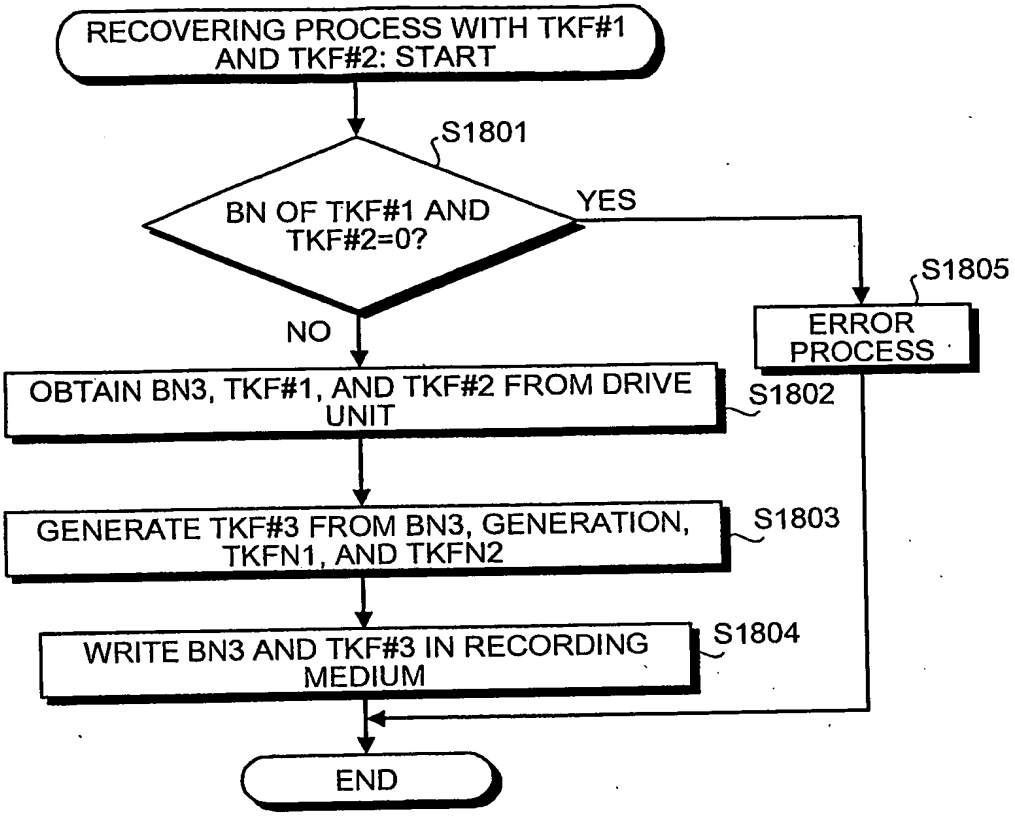
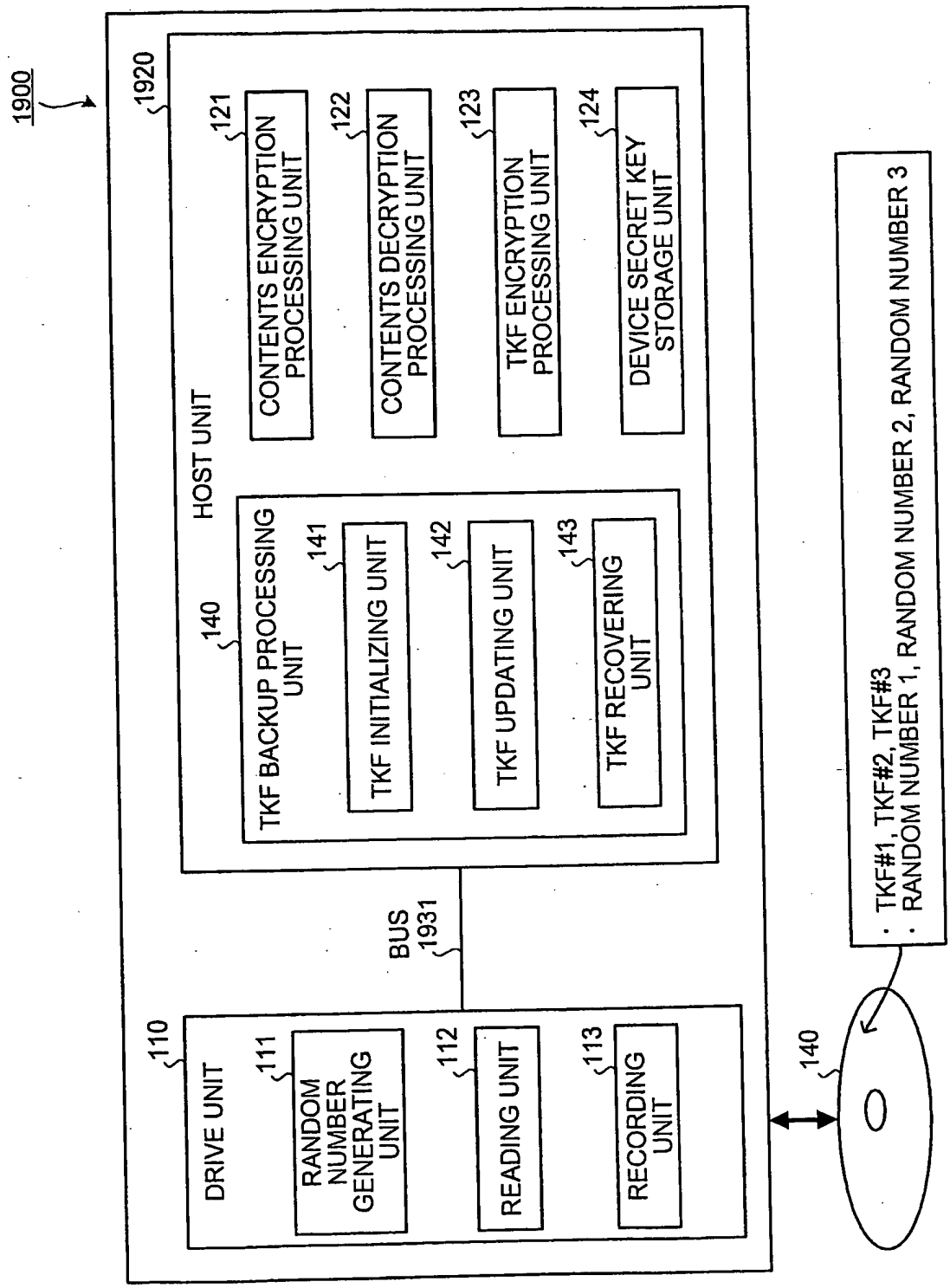

RECOVERING PROCESS WITH TKF#1 AND TKF#2: START
S1801
BN OF TKF#1 AND TKF#2=0?
YES
NO
S1805
ERROR PROCESS
OBTAIN BN3, TKF#1, AND TKF#2 FROM DRIVE UNIT
S1802
GENERATE TKF#3 FROM BN3, GENERATION, TKFN1, AND TKFN2
S1803
WRITE BN3 AND TKF#3 IN RECORDING MEDIUM
S1804
END

FIG.19


1900
1920
HOST UNIT
121
CONTENTS ENCRYPTION PROCESSING UNIT
122
CONTENTS DECRYPTION PROCESSING UNIT
123
TKF ENCRYPTION PROCESSING UNIT
124
DEVICE SECRET KEY STORAGE UNIT
140
TKF BACKUP PROCESSING UNIT
141
TKF INITIALIZING UNIT
142
TKF UPDATING UNIT
143
TKF RECOVERING UNIT
BUS 1931
110
DRIVE UNIT
111
RANDOM NUMBER GENERATING UNIT
112
READING UNIT
113
RECORDING UNIT
140
· TKF#1, TKF#2, TKF#3
· RANDOM NUMBER 1, RANDOM NUMBER 2, RANDOM NUMBER 3